Supliment al revistei „Impact strategic”

COLOCVIU STRATEGIC

Nr. 1 (168) / 2020
Indexat în
CEEOL și **ROAD**

UNIVERSITATEA NAȚIONALĂ DE APĂRARE „CAROL I”
CENTRUL DE STUDII STRATEGICE DE APĂRARE ŞI SECURITATE

AUTOMATED BORDER CONTROL SYSTEMS VS. (AVIATION) TERRORISM

András FEHÉR

Sisteme automate de control la frontieră vs. terorism (aviatic)

Rezumat: *În prezent, una dintre cele mai importante probleme este securitatea, mai ales în domeniul aviației, având în vedere vulnerabilitatea sa și efectul psihologic direct asupra oamenilor. Elementele periculoase trebuie detectate înainte de îmbarcare, deoarece neutralizarea lor ulterioară este aproape imposibilă. Una dintre posibilități este identificarea biometrică pe aeroporturi, dar acest lucru nu este încă pe deplin posibil deoarece tehnologia nu este încă disponibilă peste tot.*

În acest articol, îmi propun să analizez aplicațiile, prevalența și potențialul suplimentar al identificării biometrice pe aeroport și să explorez limitările cărora trebuie să le facem față. În opinia mea, autentificarea biometrică va contribui, cu siguranță, la securitatea călătoriilor aeriene, în timp ce va accelera și check-in-ul, dar trebuie să ținem cont de logica și realitatea tehnologică.

Cuvinte-cheie: *terorism aviatic, biometrie, identificare, aeroport, frontieră inteligentă, poartă ABC.*

Automated border control systems vs. (aviation) terrorism

Abstract: *One of the most important issues today is security, which plays an increased role in aviation, given its vulnerability and direct psychological effect on people. Dangerous elements need to be detected before boarding, as their neutralisation afterwards is almost impossible. One of the possibilities is to apply biometric identification at airports, but this is not yet fully possible due to the technology not being widespread yet.*

In this article, I examine the applications, the prevalence, and the additional potential of airport biometric identification, and explore the limitations that must be faced. In my opinion, biometric authentication is certainly going to contribute to future air travel security while also speed up check-in, but we also have to keep the logic and facts of the technology in mind.

Keywords: *aviation terrorism, biometrics, identification, airport, smart border, ABC gate.*

Introduction

'Aviation terrorism' is almost as old as aviation itself. The first officially recorded incident occurred on February 21, 1931, in Peru, when a plane got hijacked.[1]

But what is exactly aviation terrorism? The plain definition, according to Jin-Tai Choi, is: 'any terror attack carried out against the aviation industry.'[2] For terrorism, aviation is interesting because of its deterrent effect. Attacking an airplane or an airport always gets huge publicity and has a great impact on people's sense of security.[3] And the latter is what makes it particularly attractive to the terrorists. The sense of security, unlike security, is an ideal state, defined as an undisturbed state, but I am prepared for the threat and capable of averting it.

A famous description of aviation terrorism was made by the then leader of the Popular Front for the Liberation of Palestine, George Habash, in the 1960s, following a successful hijacking: 'when we hijack a plane it has a more significant effect than if we killed a hundred Israelis in battle.'[4]

Although there had been constant attacks in the previous decades, the events of 9/11 have given aviation terrorism greater attention than ever before. The incidents' nature of attacking symbolic targets has increased in scale, introducing a new element of an airplane now being not only a target, but also a means of the execution itself. All this, as we know now, has given a new impetus to the attacks against

***András FEHÉR** is a PhD candidate within Doctoral School of Security Sciences, Óbuda University from Budapest, Hungary (e-mail: feher.andras@bgk.uni-obuda.hu).*

the aviation industry. There have been many incidents in recent years, as follows:

- On October 31, 2015, an Airbus A321 plane of the Russian Metrojet airline from Sharm el-Sheikh to St. Petersburg exploded and crashed, killing 217 passengers and the crew of 7. The investigations showed that a bomb had been planted under one of the seats.[5]

- On February 3, 2016, a bomb on an Airbus A321 of Somalian airlines Daallo, flying from Mogadishu to Djibouti, exploded at a height of 4,000 meters. The plane, miraculously, landed intact despite a hole on its cabin, killing one passenger in the blast.[6]

- On March 22, 2016, two terrorists committed suicide bombings at Zaventem Airport in Brussels. Later, a terrorist detonated himself at a subway station nearby. At least 34 people died in the assassinations and 200 were injured.[7]

- On June 28, 2016, three suicide bombers began to fire at passers-by at Ataturk International Airport in Istanbul, then detonated themselves. At least 41 people died and 150 were injured.[8]

The attacks tend to become more and more creative, thanks to the security systems in the aviation industry becoming more sophisticated and able to filter out dangerous elements and threats, furthermore to the use of social media, which on the other hand simplifies communication and coordination of the attackers. Here are some failed attempts:

- On December 22, 2001, the Brit Richard Reid, intended to detonate a bomb built in the heels of his shoes on a flight from Paris to Miami. He was caught, but we bear the consequences of this in the airport Transportation Security Administration (TSA) protocol ever since.[9]

- In 2006, Al-Qaeda planned 17 simultaneous attacks on various US and Canadian aircrafts. Liquid explosives smuggled onto the planes in bottles would have been used. These attacks had been discovered in time, but as a consequence, liquids of more than 100 ml are still not allowed into the restricted areas of an airport.[10]

- On December 25, 2009, a Nigerian man, also a member of Al-Qaeda, planned to explode an Airbus A330 of Northwest Airlines, flying from Amsterdam to Detroit, using a combination of powder and liquid explosives smuggled in his underwear. The attempt failed due to the inadequate explosion of the bomb and the collaboration of other passengers, but the terrorist and two passengers were still injured.[11]

In order to fight aviation terrorism successfully, it is important to know the targets of the attacks and understand the way the terrorists think and act. As for the targets, we can name the planes themselves, the planes as the means of the action, and the airports.[12]

On this basis, the applied security measures must also be complex: to prevent terrorist equipment from being carried on board; to filter out and prevent the boarding of terrorist criminals; and to protect the airports. The last poses a serious task for law enforcement and border police authorities, both from a security conceptual and technical point of view. This is especially valid knowing that terrorist organisations prefer to use the social media and 'dark web' for communication, and that there is a tendency to recruit aviation employees for the attacks who have access to the restricted areas within the airports.[13]

As we will see, a secure way to filter out dangerous elements and thus boost security level is the widespread and automated use of biometrics. At the border crossings, if the use of a biometric pattern is required, the target person has only two options: to cooperate or to turn around (risking further proceedings due to suspicious behaviour).

1. Biometric identification

Biometric authentication is one of the most basic social functions of humans and is applied every day from birth and onwards. The child first recognises the voice, smell and face of his parents. He later identifies relatives, classmates, and friends in this way. However, technological development has only made it possible in the last few decades to establish automatic biometric identification systems. In fact, all these new developments can be traced back to the procedures used thousands of years ago. One of the oldest and most basic examples is face recognition. Since the beginning of civilisation, people have classified individuals into familiar and unfamiliar categories based on their faces. This seemingly simple task has become more and more complicated as the population grows and travel opportunities become faster and easier. Familiar faces in hitherto closed communities have been expanded with new and unknown visitors.[14]

Most human characteristics are unique. The question is whether they can be identified in the given circumstances at a reasonable cost/benefit rate or not. Such circumstance may be, for example, the state of technology or the characteristics of the specific biometrics. One of the most accurate biometric features is the DNA sequence, but it is not suitable for automated authentication in the current state of technology, both because it is slow (fastest devices run in about 10 minutes, overall process length is 90 minutes) and it is questionable whether we can be sure that only the authorised user enters his biometric sample ID. Mind that a piece of hair or dead skin falling on a computer keyboard can also be identified.

Future developments clearly point to those solutions which enable automated biometric identification, as this is the only method to truly identify the certain individual and to do it in an effective way.

Biometric systems are evaluated in different ways. The most important general aspects are as follows:

1. ‘Efficiency: Proper collection, coding and comparison of the original biometric sample is essential for the proper usability of the systems. The professional aim is to make the code as distinctive as the original, human pattern. A good algorithm selects the features within the specific pattern that really distinguish the samples from each other and overweight these features, resulting in higher identification stability and accuracy.

2. ‘Security: High number of encrypted information helps to prevent brute-force kind of attacks. The security of the biometric code can be measured by the Shannon entropy function. In addition to the algorithmic security, the reproducibility of the biometric pattern, the physical and logical security of the devices, the network communication and the monitoring software must also be examined.

3. ‘Privacy: A high level of protection of users’ personal data is required. Most importantly, the original biometric sample should not reproducible in any way from the biometric code, since in this case the same risk as storing the image of the original sample would be present. Besides the protection of the biometric data, all stored personal data must be protected likewise.’[15] Of particular importance is the EU Regulation, General Data Protection Regulation (GDPR), which entered into force on May 25, 2018.[16]

In order to use a biometric based identification system, you must meet the following criteria:

1. Universality: all persons must possess the given sample.

2. Uniqueness: any two persons should be sufficiently different in relation to the characteristic being measured.

3. Stability: the measured characteristic must be time invariant within a well-defined time interval.

4. Availability (collectability): it must be possible to collect the characteristic to be measured quantitatively.

5. Performance: the system must achieve the expected accuracy and speed depending on the operating and environmental conditions.

6. Acceptance: indicates the degree to which people are willing to accept the use of a specific biometric technology in their daily lives.

7. Misleading: The degree of risk that indicates in what extent the measured biometric feature can be distorted by an external hacker.[17]

2. Airport biometric identification

The ever-increasing international passenger traffic requires the introduction of advanced technologies that automate, simplify and accelerate border crossing.[18] Biometric passports, which can include fingerprints, face and iris samples, are increasingly being introduced on the basis of international standards.[19] Some places, such as the US and the EU, require the use of biometric passports, while in other countries it is only an option to obtain and use biometric passports for the time being. Properly designed biometric identification systems allow the security officers to focus primarily on persons of unknown risk. The special databases contain information about individuals who are dangerous to the society, so their consent to the handling of their personal data can be ignored. These databases can be supported by other specialised systems that may provide additional filtering levels as well.

The false acceptance rate of biometric systems used in border control is by far less than the false rejection rate, so it is much easier for a person trying to obstruct the control to produce an unrecognisable pattern than to force the system to believe he is someone else. If the user is not allowed to use an alternative identification method, the biometric system shall be mandatory. Authorities do not have to be ‘interested’ in users’ opinions, the only criterion is the effectiveness of the system and the security level. Of course, this does not mean that it is not advisable for authorities to develop a passenger-friendly system in their own interest, but this is not a risk factor.

2.1. Biometric Passports

The requirements for biometric passport compatibility are set out in the *ICAO 9303* document, which allows any country that requires biometric identification to handle passports from other countries.



Figure no. 1: *FastPass pilot system screen for the border guard to biometric identification of passengers arriving by passenger car*[20]

Today, migration is one of the major security challenges in the EU and also in Hungary.[21] As Lt Col Krisztina Görbe said: “There was migration, there is migration and migration will always be. In the XXI Century, one of the most significant factors of globalisation is migration, which is at the same time a complex economic, social, social, ethnic, religious phenomenon causing problems, a threat to national and regional security, and that also may be a source of well-being and maintaining the population numbers (improving statistics), being also a humanitarian solution. In summary: a category that

is difficult to handle but that needs to be managed."[22] Police Lt Col Miklós Böröcz's investigation on terrorist attacks since 2001 in Western countries revealed that these were typically committed by second or third generation immigrants, but that illegal migration and organised crime are nevertheless intertwined.[23] Consequently, the recording of relevant biometric data on immigrants would be essential in order to be able to identify criminalised individuals at an early stage.

However, the use of biometric passports raises serious data protection concerns in several aspects. In practice, these passports can be considered as a Radio Frequency Identification (RFID) Smart Card, with the biometric sample stored on a chip. These data must be adequately protected as they are read in a contactless way by any suitable reader. It is thus important to know the nature of the data (e.g. encrypted) and the form in which it is stored in the chip. At least 32 kilobytes of biometrics are stored according to the ISO/IEC 14443 standard. The above quoted ICAO document defines that since each biometric manufacturer uses different, secretly kept algorithms to template the captured samples, raw biometric samples should be stored in the passports' memory to make interoperability possible. This leaves a serious risk from a data protection point of view, since accessing a raw biometric pattern allows for a range of abuses, while accessing a template created with irreversible encryption is far less problematic.

2.2. Identification

Airport biometric identification has become possible with biometric passports becoming widespread as more and more countries make their use obligatory. Although they are yet not mandatory everywhere, in some countries, such as Israel or the US, only biometric passports are issued, the latter also made their use obligatory for all visa-free foreign travellers as well. In some countries also the ID cards are capable of storing biometric data. The introduction of biometric documents paves the way for a fully automated identification process at the airports.[24]

It is important to clarify that we are not talking about a single system that is the same all over the world, but about many unique solutions that are built around a common point. That is why one of the security factors is lost: the unique sample coding of the manufacturers. As the passports referred to in the previous paragraph have to be handled by the tools of many manufacturers, the data recorded therein had to be standardised according to ICAO 9303 document and ISO/IEC 14443 standard. The former defines the format of the biometric data and the latter defines the format of the card. This is currently being solved by storing the samples as images, which itself poses a serious risk.

At every biometric identification system in the world, from phones to access control systems, the captured pattern is normalised in each application and then transformed into a template, by the manufacturer's unique coding, that cannot be restored into its original pattern.[25] In case of the passports, this latter protection step is lost, as according to the ICAO document, the samples are recorded in JPEG and JPEG2000 formats.

At present, the identification of individuals at the airports is mostly a semi-automatic, manually done but machine-supported process.[26] The data contents of the passport are scanned with an Optical Character Recognition (OCR) the information being displayed on the screen of the officer. The system checks the passport's security features and then reads the biometrics from the chip. Parallel, the user physically enters the gate for biometric authentication (e.g. face recognition) to allow the system to compare this with the data stored in the passport. If the match is correct, the passenger can proceed. In an event of identification problems, the passenger is subjected to a more thorough human examination to clarify the reason.

There are basically two ways in which biometric systems work to store and identify a sample: 1:1 and 1:N.

1:1 refers to a system that compares a pattern presented by a person with a single stored template. Typically, the biometric data is not stored in a system database, but on an RFID card (this is usually the case with these systems).

1:N is a system that compares a presented sample with the entire database. In this case, the captured template is stored in a central database, from which the software selects the most similar template(s) that meet(s) the security criteria.

It is important to note that biometric identification never works with a 100% security, but works with probability variables.[27] The level of security is usually an adjustable feature: it can be set higher and lower based on the matching rate.

2.3. Scope and Field of Application

As seen earlier, the use of biometric identification is not yet mandatory on all airports, and the full implementation raises a number of technical and legal issues that I present among the risk factors. There are basically two purposes of biometric identification in general: positive selection and negative selection. Positive and negative expressions in this case indicate whether we wish to identify and filter out individuals who are present in a certain database or those who are not. Positive recognition means identifying individuals in the database, while negative recognition means filtering out persons not in the database.

With the current aviation systems, we see positive 1:N and 1:1 solutions, while negative ones not at all – as is the case with any access control system where the aim is to filter out all unauthorised individuals. Identification of dangerous elements is also a positive

identification, as passers-by are compared with another database that contains information about the persons being traced. In the event of a match, the security forces will take steps to withhold or arrest the suspect.

2.4. Risks and Misconceptions

There is always a risk in biometric identification systems, because they work with probabilities rather than with a 100% certainty. However, there are cumulative risk factors in airport systems, which can be categorised as: RFID chip security; biometric sample security; identification uncertainty; legal concerns. Before examining the real risks in detail, it is important to dispel the technology-related misconceptions and fears that often arise related to airport biometric identification.

The basic fear of the users is that the governments of the countries in question will possess too much information about them, their travel habits, or may steal or misuse their biometric data. However, this concern is largely unfounded, at least in context of biometrics. Governments do also currently have travel statistics (so it is possible to track which passport was used where and when even without biometrics) and also are possessing the biometric samples that are included in the passport. In Hungary, for example, when issuing an ID card or driving license, the same photograph is taken as the one required for the biometric identification system, since the biometric samples are stored as images.[28] These information could therefore also be used without issuing a passport – which is probably not to any benefit to governments. However, the concerns about personal data are not entirely groundless – as we will see below.

2.4.1. <u>Security of the RFID chip</u>

RFID chips used in passports are no different from standard RFID cards, so this is not a special development just for this application. Any attack against similar types of cards can thus also be applied to these chips. Since we are talking about contactless cards, it is enough to get close to the passport in case of a malicious attack. A way to avoid this is to store the document in a shielded case when not used (the same goes for PayPass credit cards).

2.4.2. <u>Security of the biometric sample</u>

If the passport (or its data) gets in the wrong hands, it might result in a bigger problem than in case of a traditional biometric RFID card: the sample is stored in the format specified by the ICAO document above, which can help both reproducibility and copying – and can for example be used to issue false documents.

This abuse can only be prevented by carefully storing the passport, as it is in the near future highly unlikely that the identification system will be standardised on all worldwide airports enabling designing securely coded (and thus protected) samples.

2.4.3. <u>Identification uncertainty</u>

There are two aspects to biometric identification uncertainty. On the one hand, the above-mentioned probability-based operation – the required degree of similarity between the stored and produced sample is determined by the system, but it may be affected by both external and internal factors. Furthermore, with 1:1 authentication, the algorithms examine whether the presented pattern matches the stored pattern. Theoretically, if someone, somehow manages to crack such a passport, they might either load their own data or use false data to produce fake documents: the system can only match the data identified by the sensor with the data stored on the chip.

Or the other way around: what is the response on a system level to case when a sample gets manipulated? As the only purpose of the security system is to algorithmically distinguish between the authorised and the unauthorised, based on the comparison of the live and stored samples, according to the security level you set, there is no solution at a system level to this problem. So once someone in the chain identifies himself as an authorised one, it remains so for the system.

The identification must be fast and accurate. It cannot be slower than conventional, completely human control, as it would cause passenger dissatisfaction. It also has to be accurate, as a passenger who needs to be screened separately because his biometric data 'do not match' may face serious inconvenience (depending on the skill and attitude of the airport staff).

The accuracy of face recognition technology should be regarded in this context. While iris and fingerprints can be considered reliable and durable biometric patterns, the face is far from being that – change in hairstyle alone might hook certain systems on their own, while for example wearing glasses can also be a reason for false rejection or no identification at all. This technology is also improving though, resulting in rejection rates within the range (3-5%) what users consider acceptable.[29]

2.4.4. <u>Legal concerns</u>

System security issues also raise privacy issues: can people be obligated to provide their biometrics (which by definition do not change over their lifetime) in a system where the security level cannot be guaranteed? Namely, if one of their certain biometric pattern is stolen, he might not be able to use it for other identification purposes again without having to worry about its security risk.

With the proliferation of smartphones (which are mostly also capable of biometric identification), social media and the Internet, the theft of biometric samples or data may have serious and fast-growing effects. However, there are no real legal concerns about the recognition of dangerous elements. The elimination of criminals serves the security of the whole society, who, by committing their crimes, have 'consented' (or even necessitated) to the processing of their personal data.

3. Automated border control

The Schengen Area is a 4.3 million km^2 containing 26 states today. It was established in 1995 (although the Schengen Agreement was signed on June 14, 1985) and is at present seeing about 1.3 billion crossings per annum, predicting further increase in the coming decade. These movements include tourists, commuters, transport reasons and migrates as well. Thus, a reasonable compromise of smooth, rapid process that also serves the security aspects should be targeted.[30]

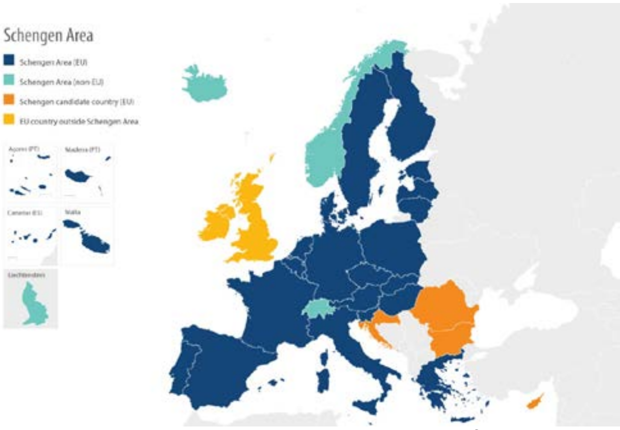


Figure no. 2: *The Schengen Area*[31]

Different incidents and phenomena, like the migrant crisis in September 2015, forced the EU to implement different steps to further strengthen the security checks of the external borders of the Schengen Area. One of these include that all of the external borders should implement biometric identification by 2021.[32] An inevitable criterion to enable this, while also an enormous challenge, is to register and record the necessary biometric samples of all travelling individuals from outside the Schengen Area by that time.

The endeavour introduces new concepts, like Smart Border, which, according to Peter Shields refers to: 'information and communication technologies that enable de-territorialized border controls. These include biometric, database and information sharing systems.'[33]

3.1. Smart Borders and the European Commission

Due to the different challenges of the past and present the EC aims to continuously improve the security level and harmonise the management of the external borders of the Schengen Area. Different programmes and projects were launched for this goal, as follows:

- February 2008: Communication from the EC identifying a range of problems and also suggesting actions to be taken. The aim is to start to develop a new and integrated external border management strategy, along four main concepts: introducing the so-called Registered Traveller Programme (RTP) status; supporting the implementation of Smart Gates; defining the Entry/Exit Registration System (EES); analyse the possibility to launch an Electronic System of Travel Authorisation (ESTA).[34]
- February 2013: the Smart Borders Package proposed by the EC goes a steps further by launching a test programme involving 12 countries and 18 border crossing points from year 2014.[35]
- January 2014: the EC launches the Automated Border Control Gates for Europe (ABC4EU), which is mainly a harmonisation project.[36] As a consequence of the above-mentioned, different ABC Gate solutions were implemented throughout Europe, and the need of harmonisation in the field of interoperability, e-passports management, biometric identification, gate design, human interface, signalling, and processes emerged. The project included 14 partner companies from seven countries forming a Consortium. It ended in 2018 and helped to the development of a new generation of ABC Gates now already in use.
- April 2016: the EC adopts a revised proposal for the Smart Borders Package, relying highly on the results of the ongoing ABC4EU project.[37]

3.2. ABC Gates

Automated Border Control (or simplified ABC) gate is by definition, according to the European Council's Regulation of the European Parliament and of the Council issued on April 6, 2016, 'a system which allows for an automated border passage by authenticating an electronic machine readable travel document (e-MRTD), establishing that the passenger is the rightful holder of the document, querying border control records and automatically determining eligibility for border crossing according to pre-defined rules and which is composed of a self-service system and an e-gate.'[38]



Figure no. 3: *ABC Gate*[39]

The ABC Gate is in practice a standalone self-service device capable of reading the biometric chip in the appropriate document, then identifying the traveller using a suitable biometric sample, such as face or fingerprint, while also matching the collected

sample to the stored one, thus verifying the user. Further features are the capability of collecting the personal information from the passport (e.g. name, sex, date of birth, passport number), checking the data to criminal record databases, and implementing physical barriers to both guide the user along the process and also withhold him in case of negative verification or identification.

The procedure performed in this process is identical to the one applied in the normal, face-to-face control, with the exception that the whole procedure can be performed as self-service in case of positive match for the samples and negative match for any undesirable criminal or legal records. In these latter cases, the user gets physically withheld by the gate until the officers take control of the process.

The potential of these solutions can be estimated from its market statistics: it was valued at $456.5 million in 2016 and is expected to reach $1,577.7 million by 2023, which might even be exceeded given for instance the EU's endeavour to introduce biometric identification on all external borders, as seen above. This is well paired with the fact that the user acceptance level of the gates is also high, mainly due to their smooth, quick and user-friendly nature.[40]

3.3. The Future

People around the world tend to use their smartphones for a widening range of purposes. From a purely communication device through a media centre and through a self-service control centre to carry out a huge variety of actions, it is now also in the scope of high security identification purposes. From a practicality point of view, the use of these devices for ID verification along a journey would be the logical choice and, according to an International Motor Vehicle Inspection Committee (CITA) report, 92% of the travellers are at least open to the idea of using them.[41]

As seen above, smooth and rapid processes are a common goal, which would obviously be served by using the mobile. The question remains that whether the hardware and software technologies could meet the high security standards targeted by the authorities. If it will be solved in the future, the possibilities of identification (e.g. multi-factor biometric authentication) and thus the achieved security level of the control can reach new heights. Smart borders may become even smarter!

3.4. An Example of eGates

To prove the potential in eGates, let us consider a specific example. The location is an international airport in Europe. Analysing a period of one month (October, 2019), a total number of 129,917 border crossings were attempted on 12 eGates, with a success rate of 82,24%. The travellers came from 17 different Schengen Area countries. The main reason of failed attempts (40,92%) were document related, followed by problems of biometric authentication (18,64%).

If we calculate with an average of 18 seconds per successful border crossing (on an eGate), the above-mentioned show that a total number of at least three officers can be saved while also improving security level by applying automated processes.

Conclusion

Aviation terrorism is given a constant attention due to its increasing nature of attacking symbolic targets and a new element of an airplane itself now possibly being also a means of the execution. The instant telecommunication applications of smart devices also contribute to aviation serving as a lucrative target for its great impact on sense of security.

As both the number of border crossings increase, though it remains to be seen what COVID-19 will leave behind as a long-term effect, and also the aims to continuously improve the security level at borders, new methods are to be found to serve these simultaneously.

The emphasis is on identifying the traveller or aviation employee in the most secure and effective way. This points at biometric identification as the only method to truly identify a certain individual.

There is a huge potential in the implementation of automated airport biometric identification, and the existing solutions are being used in fast growing number of places all over the world, and under different conditions. This fact enables both the authorities and manufacturers to improve the applied technology and processes, which at present are not yet fully mature.

While the direction is good, it would be important to resolve existing security issues and respond to emerging legal and performance concerns to achieve full automatic identification worldwide. Automated and biometrics-based multi-factor authentication performed by properly chosen and implemented systems can significantly improve the safety of airports and airplanes.

The safe introduction of the travellers' smartphones for the automated process may be the way to go, but its widespread usability is yet to be seen.

References

[1] ***, "First hijack on an aircraft", *Guinness World Records*, URL: https://www.guinnessworldrecords.com/world-records/first-hijack-of-an-aircraft.

[2] Jin-Tai Choi, Robert B. Munson, *Aviation Terrorism: Historical Survey, Perspectives and Responses*, Palgrave Macmillan UK, 1994.

[3] János Besenyő, "Low-Cost Attacks, Unnoticeable Plots? Overview on the Economical Character of Current Terrorism", *Strategic Impact*, no. 1, Centre for Defence and Security Strategic Studies, "Carol I" National Defence University, 2017, URL: https://cssas.unap.ro/en/pdf_periodicals/si62.pdf; Jack Riley, "Terrorism and Rail Security", *Testimony Series*, RAND Corporation, March 2004, URL: https://www.rand.org/content/dam/rand/pubs/testimonies/2005/RAND_CT224.pdf.

[4] Hillel Avihai, "Between Two Septembers: From the bargaining chip of Sept. 1970 to a strategic agent of Sept. 2001", *ICT's Publications*, International Institute for Counter-Terrorism, June 11, 2006, URL: https://www.ict.org.il/Article/948/between-two-septembers#gsc.tab=0.

[5] Eitan Azani, Lorena Atiyas Lvovsky, Danielle Haberfeld, "Trends In Aviation Terrorism", *ICT's Publications*, International Institute for Counter-Terrorism, August 10, 2016, URL: https://www.ict.org.il/Article/1757/trends-in-aviation-terrorism#gsc.tab=0; Will Stewart, "Russian plane crash: Bomb on tourist jet that crashed in Egypt 'was placed under a seat'", *EveningStandard*, November 23, 2015, URL: https://www.standard.co.uk/news/world/bomb-on-russian-tourist-jet-that-crashed-in-egypt-was-placed-under-a-seat-a3120741.html.

[6] ***, "Somali Authorities: Daallo Airlines A321 Explosion Caused by Bomb", *Aviation Voice*, February 9, 2016, URL: https://aviationvoice.com/somali-authorities-daallo-airlines-a321-explosion-caused-by-bomb-201602091113.

[7] Alastair Jamieson, "'Mother of Satan' Explosive Likely Used in Attack: Expert", *NBC News*, March 22, 2016, URL: https://www.nbcnews.com/card/mother-satan-explosive-likely-used-attack-expert-n543441.

[8] Itay Blumenthal, Reut Rimerman, Itamar Eichner, Roy Case, Attila Somfalvi, Amit Kotler, "Flights are resumed in Istanbul. Israelis at the airport: 'It's chaos, we're exhausted'", *ynet*, June 29, 2016, URL: https://www.ynet.co.il/articles/0,7340,L-4821867,00.html.

[9] Olga Craig, "From tearaway to terrorist - The story of Richard Reid", *The Telegraph*, December 30, 2001, URL: https://www.telegraph.co.uk/news/uknews/1366666/From-tearaway-to-terrorist-The-story-of-Richard-Reid.html.

[10] Eitan Azani, Lorena Atiyas Lvovsky, Danielle Haberfeld, *op. cit.*, August 10, 2016.

[11] Borzou Daragahi, "Bin Laden takes responsibility for Christmas Day bombing attempt", *Los Angeles Times*, January 24, 2010, URL: https://www.latimes.com/archives/la-xpm-2010-jan-24-la-fgw-bin-laden25-2010jan25-story.html.

[12] Bruce Hoffman, *Inside Terrorism*, Columbia University Press, New York, 2006.

[13] Mark Townsend, Peter Beaumont, "Russian plane crash: Calls for new era of airport security after Sinai terror", *The Guardian*, November 8, 2015, URL: https://www.theguardian.com/world/2015/nov/07/new-era-airport-security-sinai-terror.

[14] Csaba Otti, *Applicability of Biometric Access Control Systems in Mass Spaces*, PhD dissertation, Doctoral School of Security Sciences, Óbuda University, Budapest, 2019; Tibor Kovács, *Biometric Identification*, Óbuda University, Budapest, 2015.

[15] Meng-Hui Lim, Andrew B.J. Teoh, "Biometric Template Binarization", in Stan Z. Li, Anil K. Jain (eds.), *Encyclopedia of Biometrics*, Second Edition, Springer, New York, 2015.

[16] Csaba Otti, "Biometric Systems User Pattern Positioning Issues", in *DOSZ*, Spring Wind Conference, Budapest, 2016; ***, *The History of the General Data Protection Regulation*, European Data Protection Supervisor, 2019, URL: https://edps.europa.eu/data-protection/data-protection/legislation/history-general-data-protection-regulation_en.

[17] Anil K. Jain, Arun A. Ross, Karthik Nandakumar, *Introduction to Biometrics*, Springer, New York, 2011; Krisztina Földesi, *Applicability of Biometric Identification Procedures in Police Work*, PhD dissertation, Doctoral School of Security Sciences, Óbuda University, Budapest, 2017; Shimon K. Modi, *Biometrics in Identity Management: Concepts to Applications*, Artech House, Norwood, 2011; György Fialka, *The Concept, Origin, Present, Future of Financial Institution Security, Conditions and Significance of Paradigm Shift*, PhD Dissertation, Doctoral School of Security Sciences, Óbuda University, Budapest, 2016.

[18] ***, *Passenger Traffic of Hungarian Regional International Airports*, Hungarian Central Statistical Office, KTI Institute for Transport Sciences, Budapest, 2016, URL: http://www.kti.hu/trendek/magyarorszagi-regionalis-nemzetkozi-repuloterek-utasforgalma-2004-2015.

[19] János Varga, Judit Borszéki, "Smart Borders", *Military Science Review*, Volume 7, Issue 1, Faculty of Military Sciences and Officer Training, National University of Public Service, Budapest, 2014, URL: http://real.mtak.hu/107435/1/2014_1_f_varga_borszeki.pdfsequence1isAllowedy.

[20] ***, *Policy Study - Law Enforcement and Public Security*, "End of Century" Political School Foundation, Budapest, 2019.

[21] József Balla, *Security Increasing Effects of Travel and Personal Identity Documents Containing Biometric Data on Border and Public Security*, PhD Dissertation, Doctoral School of Military Sciences, National University of Public Service, Budapest, 2013.

[22] Krisztina Görbe Attiláné Zán, *The Current Situation of Hungarian Migration, Conditions and Possibilities of the Management*, PhD dissertation, "Zrínyi Miklós" National Defense University, Budapest, 2010.

[23] Miklós Böröcz, "Investigating the Relationship between Illegal Migration and Terrorism", *Terror & Protection*, Volume 2, Counter Terrorism Center, Budapest, 2015, URL: http://www.tek.gov.hu/tt_pdf/3.%20%C3%A9vfolyam%202.%20sz%C3%A1m.pdf.

[24] József Balla, *op. cit.*, 2013.

[25] Biometric identifiers (samples) are physiological characteristics related to the shape of the body. The template is the coded data derived from it that can be used to measure the match, while securing that the image of the original pattern cannot be restored from it.

[26] Stan Z. Li, Anil K. Jain (eds.), *op. cit.*, 2015.

[27] Csaba Otti, "Why Does It Fail to Operate?", in Regina Zsuzsánna Reicher, Timea Kozma, Erika Varga (eds.), *Thinking Together: The economy in practice*, Óbuda University, Budapest, 2017.

[28] ***, *Doc 9303 - Machine Readable Travel Documents*, Seventh Edition, International Civil Aviation Organization, 2015.

[29] Csaba Otti, *op. cit.*, 2019; Csaba Otti, "Classification of Biometric Access Control Systems Based on Real-Time Throughput", Proceedings of Fifth International Scientific Videoconference of Scientists and PhD students or candidates "Trends and Innovations E-business, Education and Security", University of Economics in Bratislava & Óbuda University Budapest, Bratislava, 2015.

[30] ***, *The Future of Schengen*, European Council on Foreign Relations, URL: https://www.ecfr.eu/specials/scorecard/schengen_flash_scorecard#.

[31] The source of the image is URL: https://www.europarl.europa.eu/resources/library/images/20180223PHT98530/20180223PHT98530_original.jpg.

[32] ***, *How Traveling to the Schengen Area Will Change in the Next Few Years*, SchengenVisaInfo.com, March 13, 2020, URL: https://www.schengenvisainfo.com/news/traveling-to-schengen-area-will-change-in-next-years.

[33] Esharenana E. Adomi, *Handbook of Research on Information Communication Technology Policy: Trends, Issues and Advancements*, IGI Global, Hershey, 2010.

[34] ***, *Next steps in border management in the EU*, EUR-Lex, March 18, 2008, URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=LEGISSUM:l14580.

[35] ***, *Smart Borders*, Migration and Home Affairs, European Commission, URL: https://ec.europa.eu/home-affairs/what-we-do/policies/borders-and-visas/smart-borders_en.

[36] ***, *ABC Gates for Europe: ABC4EU*, Press Release, Laurea University of Applied Sciences, March 31, 2014, URL: http://abc4eu.com/docs/Deliverable%207.20%20-%20Press%20Release%20M3%20v2.0.pdf; ***, *Automated Border Control Gates for Europe*, Press Release, Laurea University of Applied Sciences, October 30, 2015, URL: http://abc4eu.com/docs/ABC4EU_D7.23_M22%20Press%20Release.pdf.

[37] ***, *Next steps in border management in the EU*, EUR-Lex, March 18, 2008, URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=LEGISSUM:l14580.

[38] ***, *Proposal for a Regulation of the European Parliament and of the Council establishing an Entry/Exit System to register entry and exit data and refusal of entry data of third country nationals crossing the external borders of the Member States of the European Union and determining the conditions for access to the EES for law enforcement purposes and amending Regulation (EC) No 767/2008 and Regulation (EU) No 1077/2011*, European Commission, Brussels, 2016, URL: https://www.europarl.europa.eu/RegData/docs_autres_institutions/commission_europeenne/com/2016/0194/COM_COM(2016)0194_EN.pdf.

[39] Source of the image is URL: https://www.secunet.com/fileadmin/_processed_/d/a/csm_EasyGate_3_Boden_ff3f3a9391.jpg.

[40] László Kis, *Automated Border Control – Rising trend continues, experts say*, ARH Inc., March 5, 2019, URL: https://www.arh.hu/index.php/en/news/abc-gates-100-growth-in-2018.html; ***,

Automated Border Control Market by Solution Type (ABC e-Gate and ABC Kiosk), Component (Hardware, Software, and Services (Installation and Maintenance)), Application (Airport, Land Port, and Seaport), and Geography - Global Forecast to 2023, Report SE 5525, MarketsandMarkets, August 2017, URL: https://www.marketsandmarkets.com/Market-Reports/automated-border-control-market-24899883.html.

[41] ***, *op. cit.*, MarketsandMarkets, August 2017.

Bibliography

1. ***, *ABC Gates for Europe: ABC4EU*, Press Release, Laurea University of Applied Sciences, March 31, 2014.
2. ***, *Automated Border Control Gates for Europe*, Press Release, Laurea University of Applied Sciences, October 30, 2015.
3. ***, *Automated Border Control Market by Solution Type (ABC e-Gate and ABC Kiosk), Component (Hardware, Software, and Services (Installation and Maintenance)), Application (Airport, Land Port, and Seaport), and Geography - Global Forecast to 2023*, Report SE 5525, MarketsandMarkets, August 2017.
4. ***, *Doc 9303 - Machine Readable Travel Documents*, Seventh Edition, International Civil Aviation Organization, 2015.
5. ***, *Next steps in border management in the EU*, EUR-Lex, March 18, 2008.
6. ***, *Passenger Traffic of Hungarian Regional International Airports*, Hungarian Central Statistical Office, KTI Institute for Transport Sciences, Budapest, 2016.
7. ***, *Policy Study - Law Enforcement and Public Security*, "End of Century" Political School Foundation, Budapest, 2019.
8. ***, *Proposal for a Regulation of the European Parliament and of the Council establishing an Entry/Exit System to register entry and exit data and refusal of entry data of third country nationals crossing the external borders of the Member States of the European Union and determining the conditions for access to the EES for law enforcement purposes and amending Regulation (EC) No 767/2008 and Regulation (EU) No 1077/2011*, European Commission, Brussels, 2016.
9. ***, "Somali Authorities: Daallo Airlines A321 Explosion Caused by Bomb", *Aviation Voice*, February 9, 2016.
10. Adomi, Esharenana E., *Handbook of Research on Information Communication Technology Policy: Trends, Issues and Advancements*, IGI Global, Hershey, 2010.
11. Avihai, Hillel, "Between Two Septembers: From the bargaining chip of Sept. 1970 to a strategic agent of Sept. 2001", *ICT's Publications*, International Institute for Counter-Terrorism, June 11, 2006.
12. Azani, Eitan; Atiyas Lvovsky, Lorena; Haberfeld, Danielle, "Trends In Aviation Terrorism", *ICT's Publications*, International Institute for Counter-Terrorism, August 10, 2016.
13. Balla, József, *Security Increasing Effects of Travel and Personal Identity Documents Containing Biometric Data on Border and Public Security*, PhD Dissertation, Doctoral School of Military Sciences, National University of Public Service, Budapest, 2013.
14. Besenyő, János, "Low-Cost Attacks, Unnoticeable Plots? Overview on the Economical Character of Current Terrorism", *Strategic Impact*, no. 1, Centre for Defence and Security Strategic Studies, "Carol I" National Defence University, 2017.
15. Blumenthal, Itay; Rimerman, Reut; Eichner, Itamar; Case, Roy; Somfalvi, Attila; Kotler, Amit, "Flights are resumed in Istanbul. Israelis at the airport: 'It's chaos, we're exhausted'", *ynet*, June 29, 2016.
16. Böröcz, Miklós, "Investigating the Relationship between Illegal Migration and Terrorism", *Terror & Protection*, Volume 2, Counter Terrorism Center, Budapest, 2015.
17. Choi, Jin-Tai; Munson, Robert B., *Aviation Terrorism: Historical Survey, Perspectives and Responses*, Palgrave Macmillan UK, 1994.
18. Craig, Olga, "From tearaway to terrorist - The story of Richard Reid", *The Telegraph*, December 30, 2001.
19. Daragahi, Borzou, "Bin Laden takes responsibility for Christmas Day bombing attempt", *Los Angeles Times*, January 24, 2010.
20. Hoffman, Bruce, *Inside Terrorism*, Columbia University Press, New York, 2006.
21. Fialka, György, *The Concept, Origin, Present, Future of Financial Institution Security, Conditions and Significance of Paradigm Shift*, PhD Dissertation, Doctoral School of Security Sciences, Óbuda University, Budapest, 2016.
22. Földesi, Krisztina, *Applicability of Biometric Identification Procedures in Police Work*, PhD dissertation, Doctoral School of Security Sciences, Óbuda University, Budapest, 2017.
23. Görbe Attiláné Zán, Krisztina, *The Current Situation of Hungarian Migration, Conditions and Possibilities of the Management*, PhD dissertation, "Zrínyi Miklós" National Defense University, Budapest, 2010.
24. Jain, Anil K.; Ross, Arun A.; Nandakumar, Karthik, *Introduction to Biometrics*, Springer, New York, 2011.
25. Jamieson, Alastair, "'Mother of Satan' Explosive Likely Used in Attack: Expert", *NBC News*, March 22, 2016.
26. Kis, László, *Automated Border Control – Rising trend continues, experts say*, ARH Inc., March 5, 2019.
27. Kovács, Tibor, *Biometric Identification*, Óbuda University, Budapest, 2015.
28. Li, Stan Z.; Jain, Anil K. (eds.), *Encyclopedia of Biometrics*, Second Edition, Springer, New York, 2015.
29. Modi, Shimon K., *Biometrics in Identity Management: Concepts to Applications*, Artech House, Norwood, 2011.
30. Otti, Csaba, *Applicability of Biometric Access Control Systems in Mass Spaces*, PhD dissertation, Doctoral School of Security Sciences, Óbuda University, Budapest, 2019.
31. Otti, Csaba, "Biometric Systems User Pattern Positioning Issues", in *DOSZ*, Spring Wind Conference, Budapest, 2016.
32. Otti, Csaba, "Classification of Biometric Access Control Systems Based on Real-Time Throughput", Proceedings of Fifth International Scientific Videoconference of Scientists and PhD students or candidates "Trends and Innovations E-business, Education and Security", University of Economics in Bratislava & Óbuda University Budapest, Bratislava, 2015.
33. Reicher, Regina Zsuzsánna; Kozma, Timea; Varga, Erika (eds.), *Thinking Together: The economy in practice*, Óbuda University, Budapest, 2017.
34. Riley, Jack, "Terrorism and Rail Security", *Testimony Series*, RAND Corporation, March 2004.
35. Stewart, Will, "Russian plane crash: Bomb on tourist jet that crashed in Egypt 'was placed under a seat'", *EveningStandard*, November 23, 2015.
36. Townsend, Mark; Beaumont, Peter, "Russian plane crash: Calls for new era of airport security after Sinai terror", *The Guardian*, November 8, 2015.
37. Varga, János; Borszéki, Judit, "Smart Borders", *Military Science Review*, Volume 7, Issue 1, Faculty of Military Sciences and Officer Training, National University of Public Service, Budapest, 2014.

Colocviu strategic
Redactor: CS II dr. Cristian BĂHNĂREANU
Pagină web: https://cssas.unap.ro/ro/cs.htm
e-ISSN 1842-8096, 526/2020

Centrul de Studii Strategice de Apărare și Securitate
Adresă: șos. Panduri, nr. 68-72, sector 5, București
Telefon: 021.319.56.49, Fax: 021.319.57.80
E-mail: cssas@unap.ro, Website: https://cssas.unap.ro